(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000339436 A**

(43) Date of publication of application: **08.12.00**

(51) Int. Cl **G06K 19/077**
B42D 15/10
G06K 19/07
G06K 19/10

(21) Application number: **11150256**

(22) Date of filing: **28.05.99**

(71) Applicant: **HITACHI LTD**

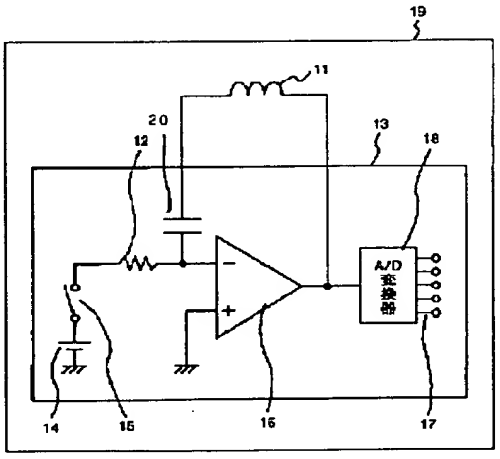
(72) Inventor: **USAMI MITSUO**
TAKARAGI KAZUO

(54) **SEMICONDUCTOR DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To obtain a card member and a semiconductor device which are reliable with respect to prevention of forgery and alteration by generating a desired signal value through the use of capacitance between a semiconductor chip and a conductor layer and separately constituted inductance.

SOLUTION: A reference voltage generator 14, an arithmetic amplifier 16 and an A/D converter 18 are mounted in a semiconductor chip 13 in a card member 19. A token device 19 constitutes a so-called integration circuit and inductance 11 by printing is constituted by combining a resistor 12, capacitance 20 between a chip and a conductor and the amplifier 16. In this integration circuit, when integration is started by a reference voltage 14 and a switch 15, analog/digital conversion is executed a fixed time later and a digital value appears at a digital terminal 17. The surface of the chip is covered with a metallic layer and capacitance between the metallic layer and the chip is essential in the integration circuit. For example, at the time of effectively using a digital output value as a key code, it can be used as a key code which cannot be reproduced by decomposing.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－339436
（P2000－339436A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　19/077		Ｇ０６Ｋ　19/00	Ｋ	２Ｃ００５
Ｂ４２Ｄ　15/10	５２１	Ｂ４２Ｄ　15/10	５２１	５Ｂ０３５
Ｇ０６Ｋ　19/07		Ｇ０６Ｋ　19/00	Ｈ	
19/10			Ｒ	

審査請求　未請求　請求項の数10　ＯＬ　（全 10 頁）

(21)出願番号　特願平11－150256

(22)出願日　平成11年５月28日(1999.5.28)

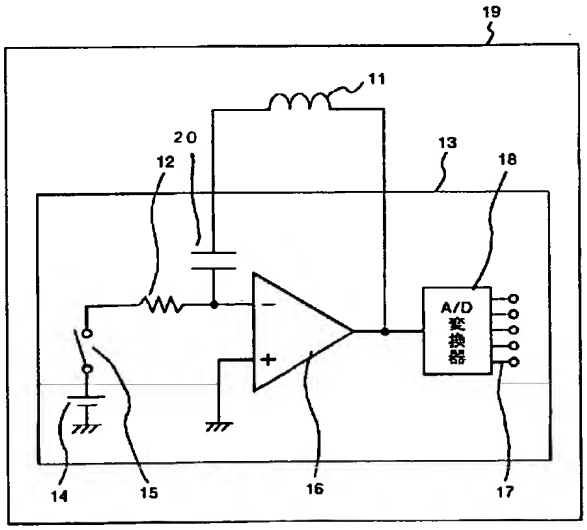
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　宇佐美　光雄
東京都国分寺市東恋ヶ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100061893
弁理士　高橋　明夫　（外１名）

最終頁に続く

(54)【発明の名称】　半導体装置

(57)【要約】
【課題】電子マネーなどに利用されるＩＣカードや紙幣などのトークンデバイスでは、分解による鍵コード盗用による偽造を防止する必要がある。
【解決手段】トークンデバイスのＩＣチップ破壊を防ぐため印刷インダクタンスと導電体とＩＣチップの間に発生する容量値によってランダムな数値を発生することによって鍵コードを発生させる。トークンデバイスが分解されたとき、自動的にインダクタンスと容量が失われ鍵コードが消失する。

図　1



1

【特許請求の範囲】

【請求項１】　半導体チップと、前記半導体チップに対向して設けられた導電体層とを少なくとも有し、前記半導体チップと前記導電体層との間の容量および前記半導体チップとは別体に構成されるインダクタンスを用いて所望信号値を発生させ得ることを特徴とする半導体装置。

【請求項２】　配線を有する基板と、前記配線を有する基板に搭載された半導体チップと、前記半導体チップに対向して設けられた第１の導電体層と、前記配線を有する基板と前記第１の導電体層との間の接着層と、前記配線を有する基板の半導体チップを搭載する面とは反対側の面に第２の導電体層とを少なくとも有し、前記半導体チップと前記導電体層との間の容量および前記半導体チップとは別体に構成されるインダクタンスを用いて所望信号値を発生させ得ることを特徴とする半導体装置。

【請求項３】　配線を有する基板と、前記配線を有する基板に搭載された半導体チップと、前記配線を有する基板の前記半導体チップに対向する面に導電体層と、前記配線を有する基板と前記半導体チップの間の接着層とを少なくとも有し、前記半導体チップと前記導電体層との間の容量および前記半導体チップとは別体に構成されるインダクタンスを用いて所望信号値を発生させ得ることを特徴とする半導体装置。

【請求項４】　所望信号値の発生は、前記半導体チップと前記導電体層間の容量と前記半導体チップとは別体に構成されるインダクタンスと演算増幅器とを少なくとも有する積分回路と、アナログデジタル変換器とを有してなされることを特徴とする請求項１、２又は３項記載の半導体装置。

【請求項５】　半導体チップを覆う導電体層を少なくとも有し、当該の半導体チップと当該の導電体層の間に発生する容量値と、当該半導体チップの外部に形成されるインダクタンスを結合した回路を用いて、ランダムな所望信号値を発生し、当該の半導体チップはこれと別体に設けたコイルによりエネルギを受信し且つ所定信号をデータ通信することを特徴とする半導体装置。

【請求項６】　半導体チップを覆う導電体層を少なくとも有し、当該の半導体チップと当該の導電体層の間に発生する容量値と、当該半導体チップの外部に形成されるインダクタンスを結合した積分回路とアナログデジタル変換器を用いて、ランダムな所望信号値を発生し、当該の半導体チップはこれと別体に設けたコイルによりエネルギを受信し且つ所望信号をデータ通信することを特徴とする半導体装置。

【請求項７】　半導体チップを覆う導電体層を少なくとも有し、当該の半導体チップと当該の導電体層の間に発生する容量値と、当該の半導体チップの外部に形成されるインダクタンスを結合した回路を用いて、所望信号値を発生し、前記インダクタンススを形成する部分と前記半導体チップは、当該半導体装置の最大の平面に交差する方向に平面的に重なる部分を有し、前記導電体層または前記インダクタンスの一部またはすべて除去したとき、当該容量値またはインダクタンスが失われ、前記半導体チップ上に形成される他の容量との連動で動作するすべてまたは一部の動作が動作しないことを特徴とする半導体装置。

2

【請求項８】　半導体チップを覆う導電体層を少なくとも有し、当該の半導体チップと当該の導電体層の間に発生する容量値と、当該の半導体チップの外部に形成されるインダクタンスを結合した回路を用いて、所望信号値を発生し、前記導電体層と前記半導体チップの間の一部または全面に導電粒子と誘電粒子とを含む接着樹脂によって充填されることを特徴とする半導体装置。

【請求項９】　半導体チップを覆う導電体層を少なくとも有し、当該の半導体チップと当該の導電体層の間に発生する容量値と、当該の半導体チップの外部に形成されるインダクタンスを結合した回路を用いて、所望信号値を発生し、且つ当該半導体装置は接触型カード部材または非接触型カード部材であることを特徴とする半導体装置。

【請求項１０】　半導体チップを覆う導電体層を少なくとも有し、当該の半導体チップと当該の導電体層の間に発生する容量値と、当該の半導体チップの外部に形成されるインダクタンスを結合した回路を用いて、所望信号値を発生し、且つ前記半導体チップをその両面または片面に補強する材料があって、当該の補強する材料の厚さは前記半導体チップの厚さよりも厚いことを特徴とする半導体装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本願発明はいわゆるＩＣカードに代表されるカード部材に関するものである。更には、本願は高度なセキュリティを有するカード部材の偽造防止に関するものである。

【０００２】

【従来の技術】従来のＩＣカードまたはトークンデバイスの偽造変造技術に関しては文献「Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ｔｈｅ ２ｎｄ Ｗｏｒｋｓｈｏｐ Ｏｎ Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｍｍｅｒｃｅ，Ｏａｋｌａｎｄ Ｃａｌｉｆｏｒｎｉａ，Ｎｏｖｅｍｂｅｒ１８－２０，１９９６」に”Ｔａｍｐｅｒ Ｒｅｓｉｓｔａｎｃｅ－ ａＣａｕｔｉｏｎａｒｙ Ｎｏｔｅ”と題して示されている。

【０００３】ＩＣカードのチップ内には、鍵と称して、取扱いが限定されるようにコードが記憶されている。このコードはメモリエリアに格納されているが、第３者により読まれてしまうと、同類のカードが偽造変造されてしまう。このコードはＩＣチップを電気的にまた物理的にまた化学的に分析されて読まれてしまう危険性があ

る。又、記憶素子（メモリ）の利用によって高セキュリティを実現する方法には次のような難点がみられた。それは、例えば、電池を常備して、何らかの電気的、物理的、化学的操作がＩＣチップにアタックされ加えられると電池による機能で、電源ダウン等でメモリが消えてしまう点であった。

【０００４】また、偽造防止のためコードを形成する従来技術として、特開昭５９－１０９３７に開示されている技術が存在する。これは、送受信アンテナ、半導体集積回路及び整流回路のばらつきに基づく電気的な諸性質の測定値を秘密保持すべきアルゴリズムに従ってコード番号にして記憶させて、偽造等に対する安全性を高めることを目的として、裏側金属化層の上方の高周波に適した誘電体（酸化アルミニウム、ポリテトラフルオロエチレン等）の上に受信アンテナを設け、半導体回路の出力部にマイクロ波送信アンテナを設け、受信アンテナから二つのダイオードを金属体面に接続して、このカードに固有の電気的な諸性質の測定値を秘密保持されるべきアルゴリズムに従ってお互いに結び合わせてコード番号を形成し、このコード番号を集積回路の中に永続的に記憶させる構成とする技術がある。

【０００５】

【発明が解決しようとする課題】これまでのカード部材、例えばＩＣカードでの高セキュリティの確保する方法には、上述のように、電池を必要とする方法が代表的なものである。従って、この方法はカード部材のコストの増大、寿命、信頼性、薄型化などの障害を生み、カード部材の普及を阻害している。

【０００６】また、偽造や変造防止の方策として、電気的な諸性質をコード化する方法が知られている。しかし、この方策は偽造や変造に対して、不十分と考えられる。即ち、電気的な諸性質に基づくコードたる対象が電気回路のばらつきとされ、ばらつきの範囲が狭く偽造されやすいこと、測定値が外部からの探索で得られやすいこと、集積回路の分解による解読に対して配慮がないことなどが、偽造や変造の前記防止技術に対する不完全さの諸要因である。

【０００７】本願発明の目的は、偽造および変造の防止に対して高信頼度なカード部材及び半導体装置を提供するものである。

【０００８】本願発明の更なる目的は、偽造および変造の防止に対して簡便な方法によって高信頼度なカード部材および半導体装置を提供するものである。

【０００９】

【課題を解決するための手段】本願発明の主な諸形態を説明し、次いで更に詳細な技術的説明を行なう。本願発明の主な諸形態を列挙すれば、次の通りである。

【００１０】本願発明の第１の形態は、半導体チップと、前記半導体チップに対向して設けられた導電体層とを少なくとも有し、前記半導体チップと前記導電体層との間の容量および前記半導体チップとは別体に構成されるインダクタンスを用いて所望信号値を発生させ得ることを特徴とする半導体装置である。

【００１１】この本願発明の第１の形態をＩＣカードに代表されるカード部材を構成した場合、次の構成がその代表的な具体的形態である。即ち、この形態は、配線を有する基板と、前記配線を有する基板に搭載された半導体チップと、前記半導体チップに対向して設けられた導電体層と、前記配線を有する基板と前記導電体層との間に接着層とを少なくとも有し、前記半導体チップと前記導電体層との間の容量および前記半導体チップとは別体に構成されるインダクタンスを用いて所望信号値を発生させ得ることを特徴とするカード部材である。以下に示す本願発明に係わる発明の諸形態もカード部材あるいはＩＣカードとして実用に供し得ることは言うまでもない。更には、本半導体装置あるいはカード部材自体ならびにＩＣカード自体を紙幣としても用いさせることが出来る。

【００１２】即ち、本願発明の第１の手段は、ＩＣチップに代表されるカード部材を補強する部材として、導電体層を有する構造において、当該カード部材内の半導体チップと当該の補強する導電体層の間に発生する容量値を利用して、各カード部材に対してランダムな数値を発生することを特徴とするＩＣカードとすることである。本形態はこのランダムな数値を用いて例えば鍵コード等を作成せんとするものである。本願発明は、半導体チップと当該の補強する導電体層の間に発生する容量値を基礎としてカードの記憶情報を設定する為、ランダムな数値によって情報の外部からの読み取りを不可能にすると共に、カードの破壊によってはその情報は破壊される形態を構成しているのである。

【００１３】本願発明の第２の形態は、配線を有する基板と、前記配線を有する基板に搭載された半導体チップと、前記半導体チップに対向して設けられた第１の導電体層と、前記配線を有する基板と前記第１の導電体層との間の接着層と、前記配線を有する基板の半導体チップを搭載する面とは反対側の面に第２の導電体層とを少なくとも有し、前記半導体チップと前記導電体層との間の容量および前記半導体チップとは別体に構成されるインダクタンスを用いて所望信号値を発生させ得ることを特徴とする半導体装置である。

【００１４】前記の第１の形態は、半導体チップの補強用の導電体層が半導体チップの片面に設けられているが、この第２の形態は、半導体チップの両面側に補強用の導電体層が設けられている例である。本例は前述の第１の形態の効果に加えて、上下２枚の補強用導電体層によってカードの外部よりの応力に対してより有効に保護されている。

【００１５】本願発明の第３の形態は、配線を有する基板と、前記配線を有する基板に搭載された半導体チップ

と、前記配線を有する基板の前記半導体チップに対向する面に導電体層と、前記配線を有する基板と前記半導体チップの間の接着層とを少なくとも有し、前記半導体チップと前記導電体層との間の容量および前記半導体チップとは別体に構成されるインダクタンスを用いて所望信号値を発生させ得ることを特徴とする半導体装置である。

【００１６】即ち、本願発明のこの形態はＩＣチップに接続するいわゆる基板パターンとなる導電体層を有する構造において、当該のＩＣチップと当該の基板パターンの間に発生する容量値を利用してランダムな数値を発生することを特徴とするＩＣカードとすることである。

【００１７】この第３の例は、半導体チップを搭載する基板に基板パターンが導電体層で形成されている例である。この基板パターンは半導体チップに接触する構成を取っている。従って、前述の諸形態に比較して基板に導電体層を形成することで本願の目的を達成することが出来、簡便な方法である。

【００１８】本願発明の第４の形態は、所望信号値の発生は、前記半導体チップと前記導電体層間の容量と演算増幅器と前記半導体チップとは別体に構成されるインダクタンスを用いてを少なくとも有する積分回路と、アナログデジタル変換器とを有してなされることを特徴とする前記第１、２又は３の形態のカード部材である。

【００１９】本形態は、半導体チップと当該の補強する導電体層の間に発生する容量値を情報の基礎として積分回路が動作する。従って、カードに記憶された記憶情報は、外部からの読み取りを不可能にすると共に、カードの破壊によってはその情報は破壊される形態を構成しているのである。

【００２０】前記の課題を解決する第５の形態はＩＣチップをカバーする導電体層を有する構造において、当該ＩＣチップと当該の導電体層の間に発生する容量値と、当該ＩＣチップの外部に形成されるインダクタンスを結合して、各カード部材に対してランダムな数値を発生し、当該ＩＣチップは別に設けるコイルによりエネルギ受信とデータ通信することを特徴とする半導体装置とすることである。

【００２１】前記の課題を解決する第６の形態はＩＣチップをカバーする導電体層を有する構造において、当該ＩＣチップと当該の導電体層の間に発生する容量値と、当該ＩＣチップの外部に形成されるインダクタンスを結合してランダムな数値を発生し、当該のランダムな数値は当該の容量とインダクタンスを結合した積分回路とアナログデジタル変換器を利用して発生することを特徴とする半導体装置とすることである。

【００２２】前記の課題を解決する第７の形態はＩＣチップをカバーする導電体層を有する構造において、当該のＩＣチップと当該導電体層の間に発生する容量値と、当該ＩＣチップの外部に形成されるインダクタンスを結

合してランダムな数値を発生し、当該のインダクタンスを形成する部分と当該ＩＣチップは平面的に重なる部分があって、当該導電体層または当該インダクタンスを一部またはすべて除去したとき、当該の容量値またはインダクタンスが失われ、そのために、ＩＣチップ上に形成される他の容量との連動で動作するすべてまたは一部が動作しないことを特徴とする半導体装置とすることである。

【００２３】前記の課題を解決する第８の形態はＩＣチップをカバーする導電体層を有する構造において、当該のＩＣチップと当該の導電体の間に発生する容量値と、当該のＩＣチップの外部に形成されるインダクタンスを結合してランダムな数値を発生し、当該の導電体層とチップの間には導電粒子と誘電粒子を含む接着樹脂によって一部または全面に充填されることを特徴とする半導体装置とすることである。

【００２４】前記の課題を解決する第９の形態はＩＣチップをカバーする導電体を有する構造において、当該のＩＣチップと当該の導電体の間に発生する容量値と、当該のＩＣチップの外部に形成されるインダクタンスを結合してランダムな数値を発生することを特徴とする半導体装置で当該の半導体装置は接触型または非接触型ＩＣカードまたは紙幣であることを特徴とする半導体装置とすることである。

【００２５】前記の課題を解決する第１０の形態はＩＣチップをカバーする導電体を有する構造において、当該ＩＣチップと当該の導電体の間に発生する容量値と、当該ＩＣチップの外部に形成されるインダクタンスを結合してランダムな数値を発生することを特徴とする半導体装置で当該ＩＣチップを両面または片面に補強する材料があって、当該の補強する材料の厚さは当該のＩＣチップよりも厚いことを特徴とする半導体装置とすることである。

【００２６】

【発明の実施の形態】図１は本願発明の実施の形態の例の半導体チップ部分の回路の構成を示している。符号１３は当該カード部材１９内の半導体チップを示しているが、このチップ１３内に、基準電圧発生器１４、演算増幅器１６、Ａ／Ｄ変換器１８などが搭載されている。半導体チップとしては、シリコン基板に上述の様に増幅器や抵抗など各種所要素子を形成した通常のもので良い。また、この半導体チップに対向して配置される基板としては、例えば厚さが０．１ｍｍ～１．０ｍｍ程度のＰＥＺ、ＰＶＣあるいはポリカーボネイトなど、各種有機プラスッチク膜を使用することが出来る。

【００２７】ここで、符号１９は具体的にはトークンデバイスの例を示している。このトクンデバイス（１９）はいわゆる積分回路を構成する。即ち、この積分回路は、印刷によるインダクタンス１１は、抵抗１２とチップと導電体の間の容量２０と演算増幅１６と組み合わさ

れて構成されてる。

【００２８】この積分回路は基準電圧１４とスイッチ１５によって積分が開始されると、一定時間後にアナログデジタル変換が行れ、デジタル出力端子１７にデジタル値が出現する。これらの回路は半導体技術によって、チップ１３の中に入れられて形成される。そして、このチップの表面にはメタル層がカバーされる。

【００２９】このような構造は当該カード部材のセキュリティ確保の為に、下記のような数々の利点を有している。本願発明において、特に重要なことは、前記半導体チップ表面のメタル層の形成と、このメタル層とチップの間の容量を用いて積分回路を構成してあることである。このことを利用することによって、例えば鍵コードの再現を不可能とする。

【００３０】前記メタル層とチップの間の容量が積分回路では必須となるので、仮にこのメタルカバーがはずされると容量が消えてしまい、積分回路が動作しなくなる。またメタルとチップの間には、一方向性の回路たとえば、ショート回路があって、オープンになると次に電源が入ると他の回路を動作不能とする仕組みなどを入れれば、容量を他の方法で知っても再現不能となる。また、デジタル出力値は鍵コードとして有効に使用されれば、分解によって、再現不能な鍵コードとして使用することができる。補強メタルは本来ＩＣカードのチップ割れ防止に有効に使われるものであり、これらのことより、簡便でセキュリティの高いＩＣカードが実現できる。

【００３１】図２は本発明の別の実施の形態の平面図を示している。

【００３２】ＩＣカード２１の中には、薄型のチップ２２があり、チップからは接続線によって、アンテナコイル２３に接続されている。図２では主要構成部品の配置のみを模式的に示している。図２では補強メタル２４はチップ２２の下部に設けられたものを示している。チップ２２からは接続線２５によって、アンテナまたは接触端子２３に接続されている。このアンテナまたは接触端子２３をいずれを選択するかによって、いわゆる接触型、あるいは非接触型のＩＣカードないしはカード部材となる。

【００３３】ＩＣカードは機械的強度が応用範囲を決めてしまうことがある。すなわち、高額を扱う金融カードに於いては、ごく一般的な用途のＩＣカードより、ＩＣカードの信頼性が強く要求されている。このため、薄型チップに厚いメタルを補強または裏打ちすることによって、機械的強度を強くすることを本発明者は見出している。従って、このような強度が強いＩＣカードの応用範囲では、高いセキュリティが要求されている。

【００３４】セキュリティの範囲はいろいろあるが、チップの中にある電気的に書き込み可能なメモリ（ＥＥＰＲＯＭ）は各種の分析装置を使えば、メモリの内容を読みだすことが可能である。このメモリの中には暗号として必要な鍵コードが入っているので、このことは、鍵コードが読まれてしまうことを意味している。一般に、暗号技術によりシステムの信頼性が確保されると信じこまれるので、暗号の鍵コードがいったん破られて悪用されると、致命的損害規模にのぼると予想され、影響範囲がきわめて大きい。本発明では、このような事態を避ける方法を提案する。

【００３５】図３は本願発明の係わる印刷によるインダクタンスの配置を示している。図３は、印刷によって形成されたインダクタンス７２がＩＣチップ７１の上に印刷されていることを示す。尚、図３はカード部材におけるこの関係のみを示している。又、印刷によって形成されたインダクタンスを単に印刷インダクタンスと以下略称する。

【００３６】図４は本願発明の別な実施の形態の例の断面図を示している。この例は、半導体チップの上下を補強材２枚で挟んだ形態の例である。

【００３７】図５は、本発明の別の実施の形態の断面図を示している。この例は、半導体チップを１枚の補強材で補強した例である。以下には図４の例をもって詳しく説明するが、補強材以外の基本的な事項は図５の例においても同様である。従って、その詳細説明は省略する。

【００３８】基板３８には電極３１を介して半導体チップ３２が搭載されている。一般には、チップ３２は接着剤３４によって基板３８に接着されている。こうして準備された諸部材は補強材４２および別な補強材４３によって補強されている。補強材の具体的材料としては、タングステン、ステンレスなどを挙げることが出来る。符号３３は本願発明に係わる印刷インダクタンスで、補強材４２に印刷で形成されている。印刷インダクタンス自体は通例の技術で十分である。このようにして準備された積層体が樹脂、例えば有機樹脂４５でパッケージングされる。有機樹脂の代表例としてＰＥＴ（ポリエチレンラレフタート）を挙げることが出来る。

【００３９】また、半導体チップ３２は当該カード部材の上面と下面との中立面４４に配置されることが好ましい。この形態は、カードの外部からの応力に対してより安定な、低ストレスな配置であると言うことが出来る。中立面の位置は概ね±５％程度のずれの範囲が好ましい。尚、この半導体チップのカード部材中の位置に関しては、直接のこの例に限らず、本願に係わるカード部材の全般の諸形態に対して言い得ることである。

【００４０】基板３８上の電極３１は薄型のＩＣチップ３２にあるチップ上の電極３５と導電粒子３７によって接続されている。導電粒子は接着剤３４の中に分散して存在している。薄型チップの上には印刷インダクタンス３３で接続されている。また、界面３９の下には、基板３８と接して、他の補強材４３と接続されている。上側にも補強材４２がある。補強メタルはさまざまな接着層

をもって接続することが可能であり、たとえば、強誘電体粒子４１を分散した接着剤や、厚さが自由に設定できる接着剤やシート、誘電率が異なる接着剤などが使用出来る。

【００４１】本願発明においては、前述したように、前記半導体チップ表面の形成した補強材たるメタル層を形成し、このメタル層とチップの間の容量を用いることが肝要である。各カード部材の有する前記容量値を、メタル層とチップの間の間隔やこの間に挿入される接着層の誘電率などの選択によって、有意にさまざまな値を設定することが出来る。接着層の誘電率は、その母剤の材質や、接着層の厚さ、この母剤に添加する添加物、この添加物の表面の状態、例えば前述のように強誘電体粒子４１を分散させることによって、ランダムの容量値を発生する要因はさまざまである。従って、この容量値は任意なランダムな値に設定することが出来る。

【００４２】こうして、半導体チップとメタル層の間の容量値をさまざまなばらつきに設定することができる。このことにより、事前にチップとメタルの間の容量を把握することが困難となす。従って、非破壊にはカード部材に内臓された情報を把握するのは不可能である。更には、半導体チップ上の解析をするために、前記補強用メタル層を外してしまうと容量が消失してしまうことになる。従って、カード部材を破壊しては、カード部材に内臓された情報、例えば、鍵コード等の解析は不可能となる。

【００４３】尚、実用的なＩＣカードの形態として、各部材の厚さ等は次の通りである。

【００４４】半導体チップ３２の厚さは１１０μｍ以下が多用される。更に、その厚さはより多くは通例５０μｍ～１１０μｍが用いられる。電極層３１の厚さは通例２０μｍ～３０μｍ、基板３９の厚さは通例１０μｍ～１００μｍ、補強用メタル層３３、３６の厚さは通例各々１０μｍ～２５０μｍ、接着剤層３４の厚さは通例５μｍ～５０μｍ、程度である。本願発明の他の諸形態においても、こうした各部材の厚さ採用される。

【００４５】実際的な観点で、カードや半導体チップの厚さは次の範囲より多用される。即ち、ＩＣチップが破壊しない、あるいはその応力が実質的に半導体チップの動作に影響がない範囲が当然選択されるのである。例えば、カードが０．７６ｍｍの時はＬＳＩの厚さは１１０ミクロン以下とすることが望ましい。カードの厚さが、０．５ｍｍの時は１９ミクロン以下がより望ましい。カードが０．２５ｍｍの時はＬＳＩの厚さは４ミクロン以下の厚さがより望ましい。勿論、ＬＳＩを極限まで薄くしたほうが、信頼度は大きく向上する。

【００４６】図６は本発明の別の実施の形態の平面図を示している。尚、この図ではパッケージングの樹脂は省略されている。本例はチップ６２に対向する基板に導電体のパターン６５を形成して、チップ６２と導電体のパターン６５の間の容量を本願発明に係わる容量として用ようとするものである。これまでの例と同様に外部からの情報の読み出しを防止することが出来る。図７は図６のＡＡでの断面を示す図である。６２は基板、６４は基板上の電極、６５は本例に係わる金属パターン、６２は半導体チップ、６８は半導体チップの電極、６７は導電粒子である。

【００４７】グランド端子６１はチップ６２の表面にあって、基板上のパターン６５と接続されている。また、同じくチップ上には、コイル端子６３があって、コイルライン６４と接続されている。このような形態であると、基板上のパターンはほぼチップ全面にグランドのパターンをおくことができる。従って、チップとこのパターンの間には容量を設定することが可能となる。今、このパターンをグランドとして扱ったが、設計によっては自由な電位またはインピーダンス端子とすることが可能である。このパターンとチップは接着剤などを介して面と面が並行と向かいあうことが可能となるので、その間に強誘電体の粒子を分散すれば、容量値を分散することが可能となる。この例では、非接触ＩＣカードの例を示しているが、接触型ＩＣカードにおいても同様な例によって実現することができる。また、基板上のパターン６５はチップ上のパターンと組み合わせることによって、容量をばらつかせることは可能である。またレーザ技術によっても、ランダムな形態を形成することができる。

【００４８】図８は本願発明をシステムの実施の形態の例を示す概念図である。ＩＣカード５２の中にはチップ５１があって、リーダライタ５３とデータのやりとりを行う例を示している。リーダライタのなかには、コントロールプロセッサ５４およびデータベースとなる磁気ディスク５５などが存在する。

【００４９】まず、リーダライタ５３からＩＣカード５２に対して、ＩＤの問い合わせが行われる。

【００５０】まず、リーダライタ５３からＩＣカード５２に対して、ＩＤ（ＩＤＥＮＴＩＦＩＣＡＴＩＯＮ）、例えば、当該カードの管理責任者を特定する為の氏名コードまたは認識コードの問い合わせが行われる。図５にはこの状態を（１）として示した。この氏名コードまたは認識コードはＩＣチップの中にある所定のエリアに格納されている。　ＩＣカードは氏名コードをリーダライタに返答する。リーダライタはデータベース５３にある氏名コードを検索して、データベース上の鍵コードを獲得する。

【００５１】リーダライタは乱数をＩＣカードに送る。この乱数は、例えばリーダライタ内のＭＰＵで回路的に発生される。ＬＡＮ等でサーバ側から乱数を供給することも出来る。

【００５２】ＩＣカードは、乱数を受け取った時点で、コマンドによってリーダライタから指示を受け、乱数を鍵コード発生部に従って発生した鍵コードによって暗号

化した乱数を作成する。

【００５３】一方、リーダライタはＩＣカードと同様にデータベースから得た鍵コードを使用して、ＩＣカードへ送ったのと同じ乱数を暗号化する。これによって得られた暗号化された乱数の結果と先のＩＣカードからの暗号化された乱数を照合して、一致がとれれば、ＩＣカードとリーダライタの相互認識が完了して、ＩＣカードの正当性が認められる。

【００５４】このようにして、本システムでは、この鍵コードがリーダライタに伝えられるとリーダライタは磁気ディスクの中のＩＤを検索して、正しく登録された鍵コードによるＩＤであると認識する。

【００５５】生成されたＩＣカードの鍵コード（ＩＤコード）は、氏名コードまたは認識コードとともにデータベースに格納される。

【００５６】生成された鍵コードは電子マネーとしてＩＣカードが使用される時の本人認証や偽造チェックやＩＣカードとリーダライタの相互認証に使用することが出来る。

【００５７】上記システムは、例えば、一般商店での支払や、チケットの購入、定期券での改札、免許証のチェック、テレフォンカードによる電話等々多くの分野に応用することが出来る。

【００５８】本願発明におけるこのＩＤは、ＩＣカードの本発明で実施される半導体チップとメタル間の容量を利用し、チップ内の抵抗値と演算増幅器によって積分回路を用いて、その後、数値変換して、鍵コードを発生したものを利用することに特徴がある。

【００５９】ＩＣカードは氏名コードをリーダライタに返答する。即ち、この鍵コードがリーダライタに伝えられるとリーダライタは磁気ディスクの中のＩＤを検索して、正しく登録された鍵コードによるＩＤであると認識する。

【００６０】このリーダライタ５３からの問い合わせが、途中の経路によって盗聴されるおそれがあるときは、暗号技術を用いて行われることが一般に行われる。同時にＩＣカードのチップ内のＥＥＰＲＯＭに書き込まれている、例えば名前や住所、電話番号などが同時にリーダライタに転送されるが、鍵コードと組み合わせれば、同種の組合せは鍵コードのビット数を確保すれば、出現することはない。こうして、セキュリティを確保することが可能となる。実用上、前記のビット数は６４ビット以上が有用である。

【００６１】例えば、図１の回路構成を用いて本願発明に係わる容量を用いて諸コードに変換する方法を例示する。電源１４によって電圧を発生させ、アンプ１６とインダクタンス１１、容量２０で構成される積分回路で増幅し、Ａ／Ｄ（アナログデジタル）変換器１８によってデジタルに変換し、出力端子１７に電圧発生させる。この場合、当該積分回路の出力値は容量、インダクタンス、および抵抗の関数（Ｖ（ｔ）＝ｆ（Ｃ、Ｌ、Ｒ））である。従って、これまでの説明から明らかなように容量値を各半導体装置に個別のランダムな値とせしむると、前記出力値も各半導体装置に個別のランダムな値となすことが出来る。

【００６２】前記出力端子１７よりの電気信号を乱数発生回路に入力し、乱数を発生させる。

【００６３】この乱数をコードとする。例えば、名前をコード化するとする。Ａ／Ｄ変換器が９ビットであるとすると、２進数で１１１１１１１１１（１０２３）となる。

【００６４】このＡ／Ｄ変換されたコードは、リーダライタ（ＲＷＵ＝Ｒｅａｄｅｒ－Ｗｒｉｔｅｒ Ｕｎｉｔ）により、カード外に読み出され、暗号処理され、例えば、１０１０１０１０１となる。その後、この暗号処理されたコード１０１０１０１０１はシステムの要請に応じる。例えば、このデジタル信号はリーダライタ側に送信される。

【００６５】しかし、本願発明においては、所望信号を、積分回路で増幅し、Ａ／Ｄ（アナログデジタル）変換器１８によってデジタル信号に変換する場合、半導体チップと所定の導電体層との間に生ずる容量と、当該半導体チップの外部に設定されるインダクタンスを用いた積分回路を用いる為、そのＩＣカード固有の容量値およびインダクタンスに基づく積分がなされることとなる。こうして、当初の名前の信号が暗号処理によって、そのＩＣカードに固有の暗号処理がなされることとなる。従って、外部からは、暗号処理後デジタル信号によって当初の名前の信号は解読が不可能となる。

【００６６】ＩＣカードとリーダライタの間の交信方式は種々考えられ、接触式または非接触式などの方式が存在する。従って、これらの方式の差異があっても、本願発明のチップとメタル間で発生する容量を用いる方法は共通に使用することが可能である。尚、接触式または非接触式などの方式自体は通例のものを用いれば十分である。

【００６７】ここで、本願発明に係わるカード部材ないしは半導体装置の適用について説明する。

【００６８】ＩＣカードは諸システムのサポートによって、諸目的に実用化されるが、ＩＣカードに搭載される鍵コード等がシステムのデータベースに登録されていると、安全に運用し、認証システムに使用することが出来る。この登録コードとしては、ＩＤナンバー、名前、暗証ナンバー、個人の属性データ、サービスの来歴データ、クレットナンバー、口座情報、信用レベルなどとして、応用することが出来る。

【００６９】本願に係わる鍵コードは極めてばらつきを持って実現されるので、同じコードとなる確率は極めて小さい。従って、同じカードが作成されることは極めて困難とある。

【００７０】また、本願発明のＩＣカードの鍵コードが暗証コードまたは生物学的特徴コードと結びついて、本人認証を行なうために用いることも出来る。本願発明のより、効果的な用い方である。

【００７１】例えば、コードとして生物学的特徴コード（手の平をパターン化した掌紋コード、指紋をデータ化した指紋コード、人体から発生する匂いに基づく匂いコード、顔の形をパターン化した顔コード、声の情報をパターン、デジタル化するあるいは分析値に基づく音声コード、静脈のパルスをパターン化した静脈コード、目の色や形をパターン化した瞳孔コード、ＤＮＡをパターン化したＤＮＡコード）などを用い得る。即ち、上記バイオメトリクスで考えられるその人の個人コードを用いることによって、より個人認証を安全に実現することが出来る。

【００７２】上記システムは、例えば交通、運輸、金融などの多くの分野に応用することが出来る。これらの例は、例えば、一般商店での支払い、チケットの購入、定期券での改札、免許証のチェック、テレホンカードによる電話等等多くの分野に適用出来る。これにより、商店ではカードをかざすだけで商品を買うことが出来る。又、映画館に行くときその都度並んでキップを買うことなく、入場出来る。旅館の予約や精算が出来る。インターネットで雑誌の必要な部分を複写して料金を支払うことが出来る。有料放送ＴＶで所望の放送を鑑賞できる。マンツーマンの英会話の料金の支払いが出来る。クレジットカードの代わりに使え、かつ小金の決済にも使用することが出来る。更には、コンピュータシステムや場所のアクセスにも使用することが出来る。

【００７３】多額な金額を取扱うＩＣカードまたは高額紙幣では、偽造変造を防止する有効な形態が必要である。本発明により、ＩＣカードの偽造変造に対して有効に防御できる方法を経済的に提供することが可能となる。お互いに対向する半導体の電極と基板の電極間の誘電体の材料、厚さ形状等を変更して容量値をＡ／Ｄ変換し、鍵コードとすると容量値がランダム値となり、これを暗号の鍵コードと使用するので偽造変造ができなくなる。またＩＣカードを分解したり、電気的測定をはかると再現不能となり、偽造変造が不可能となる。

【００７４】以上、詳細に説明した通り、本願諸発明によれば、高信頼度なカード部材の偽造変造防止技術を提供することが出来る。また、高セキュリテイ確保のための所望信号を得るに容量を利用する為、安価に製造することができ、複雑な装置、部品をも必要とせず、極めて経済的である。また、その技術からみて長寿命である。このように、広くＩＣカードが電子マネーなど現行の貨幣機能を有するデバイスとして使われるときの高度の偽造防止技術として極めて有用である。

【００７５】

【発明の効果】本願発明は、より高度なセキュリティを有するカード部材を提供することが出来る。

【図面の簡単な説明】

【図１】図１は本願発明の例を示す回路構成図である。

【図２】図２は本願発明の主要構成部材の配置の例を示す平面図である。

【図３】図３は本願発明の印刷アンテナの例を示す平面図である。

【図４】図４は本願発明の実施の形態を示す断面図である。

【図５】図５は本願発明の実施の形態を示す断面図である。

【図６】図６は本願発明の別な実施の形態を示す平面図である。

【図７】図７は図６の実施の形態の断面図である。

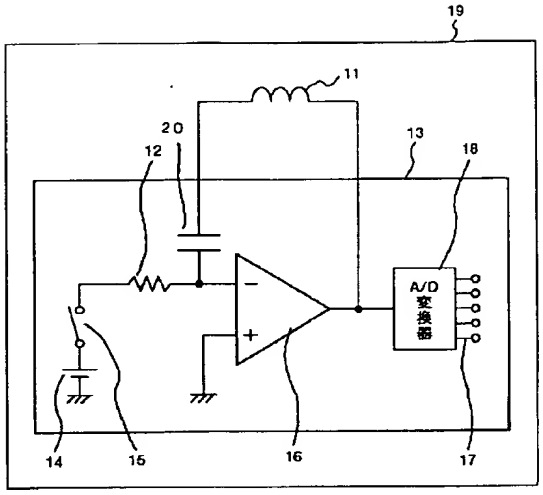
【図８】図８は本願発明のカード部材の適用の例を示すシステム概略図である。

【符号の説明】

１１…印刷によるインダクタンス、１２…抵抗、１３…チップ、１４…基準電圧、１５…スイッチ、１６…演算増幅器、１７…デジタル出力端子、１８…Ａ／Ｄ変換器、１９…トークンデバイス、２０…チップと導電体の間の容量、２１…ＩＣカード、２…チップ、２３…アンテナコイル、７１タンス、３１…基板上の電極、３２…ＩＣチップ、３３…印刷インダクタンス、３４…接着剤、３５…チップ上の電極、３７…導電粒子、３８…基板、３９…界面、４１…誘電粒子、４２…補強材、４３…他の補強材、５１…チップ、５２…ＩＣカード、５３…リーダライタ、５４…コントールプロセッサ、５５…磁気ディスク、６１…グランド端子、６２…チップ、６３…コイル端子、６４…コイルライン、６５…基板上のパターンである。

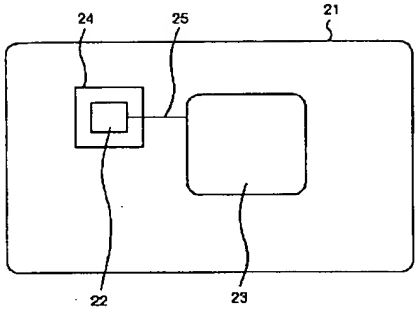
【図１】

図 1



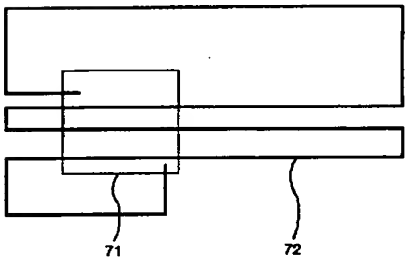
【図２】

図 2



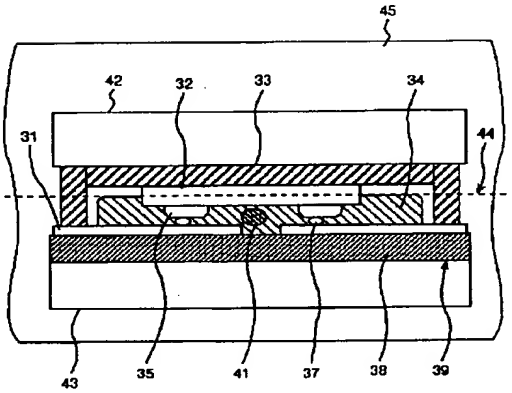
【図３】

図 3



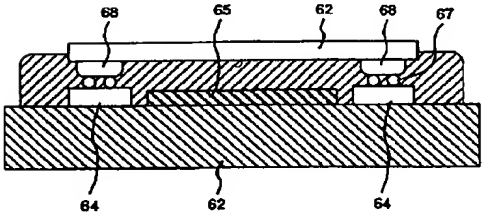
【図４】

図 4



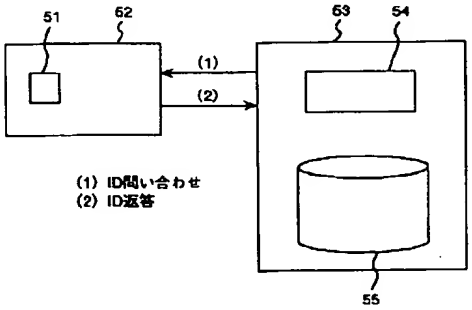
【図７】

図 7



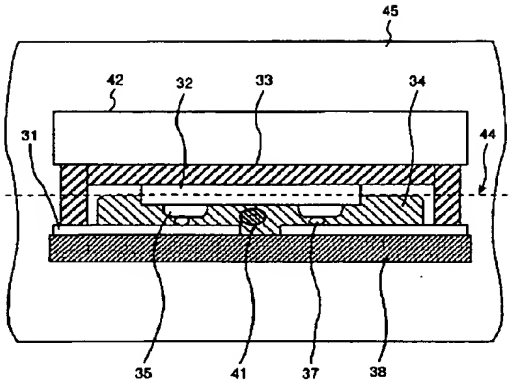
【図８】

図 8



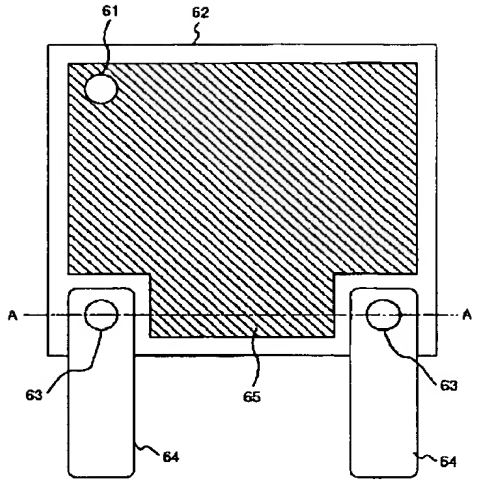
【図５】

図 5



【図６】

図 6



フロントページの続き

Ｆターム(参考) 2C005 MA01 MA10 MB02 MB05 MB07
MB08 MB10 NA09 PA18 PA25
PA27 SA02 SA15 TA21 TA22
5B035 AA14 BA05 BB09 BC01 CA01
CA23 CA38